

Constructing Linear Codes with Good Joint Spectra

Shengtian Yang, Yan Chen, Thomas Honold, Zhaoyang Zhang, and Peiliang Qiu

Department of Information Science & Electronic Engineering

Zhejiang University

Hangzhou, Zhejiang 310027, China

{yangshengtian, qiupl418, honold, ning_ming, qiupl}@zju.edu.cn

Abstract—The problem of finding good linear codes for joint source-channel coding (JSCC) is investigated in this paper. By the code-spectrum approach, it has been proved in the authors' previous paper that a good linear code for the authors' JSCC scheme is a code with a good joint spectrum, so the main task in this paper is to construct linear codes with good joint spectra. First, the code-spectrum approach is developed further to facilitate the calculation of spectra. Second, some general principles for constructing good linear codes are presented. Finally, we propose an explicit construction of linear codes with good joint spectra based on low density parity check (LDPC) codes and low density generator matrix (LDGM) codes.

I. INTRODUCTION

A lot of research on practical designs of lossless joint source-channel coding (JSCC) based on linear codes have been done for specific correlated sources and multiple-access channels (MACs), e.g., correlated sources over separated noisy channels (e.g., [1]), correlated sources over additive white Gaussian noise (AWGN) MACs (e.g., [2]), correlated sources over Rayleigh fading MACs (e.g., [3]). However, for transmission of arbitrary correlated sources over arbitrary MACs, it is still not clear how to construct an optimal lossless JSCC scheme. In [4], we proposed a lossless JSCC scheme based on linear codes for MACs, which proved to be optimal if good linear codes and good conditional probabilities are chosen. Figure 1 illustrates the mechanism of our scheme in detail. Using the code-spectrum approach established in [4], we found that a good linear code for our JSCC scheme is a code with a good joint spectrum. Hence, to design a lossless JSCC scheme in practice, a big problem is how to construct linear codes with good joint spectra. In this paper, we will investigate the problem in depth and give an explicit construction of linear codes with good joint spectra based on sparse matrices.

In the sequel, symbols, real variables and deterministic mappings are denoted by lowercase letters. Sets and random elements are denoted by capital letters, and the empty set is denoted by \emptyset . Alphabets are denoted by script capital letters. All logarithms are taken to the natural base e and denoted by \ln . The composition of the functions f and g is denoted by $f \circ g$, where $(f \circ g)(x) \triangleq f(g(x))$. The indicator function is denoted by $1\{\cdot\}$. The cardinality of a set A is denoted by $|A|$.

¹This work was supported by Zhejiang Provincial Natural Science Foundation of China (No. Y106068), by the National Natural Science Foundation of China (No. 60602023, 60772093), and by the National High Technology Research and Development Program of China (No. 2006AA01Z273, 2007AA01Z257).

For any random elements F and G in a common measurable space, the equality $F \stackrel{d}{=} G$ means that F and G have the same probability distribution.

II. BASICS OF THE CODE-SPECTRUM APPROACH

Before investigating the problem of constructing good linear codes, we first need to briefly introduce our “code-spectrum” approach established in [4], which may be regarded as a generalization of the weight-distribution approach (e.g., [5]).

Let \mathcal{X} and \mathcal{Y} be two finite (additive) abelian groups. We define a *linear code* as a homomorphism $f : \mathcal{X}^n \rightarrow \mathcal{Y}^m$, i.e., a map satisfying

$$f(x_1^n + x_2^n) = f(x_1^n) + f(x_2^n) \quad \forall x_1^n, x_2^n \in \mathcal{X}^n$$

where \mathcal{X}^n and \mathcal{Y}^m denote the n -fold direct product of \mathcal{X} and the m -fold direct product of \mathcal{Y} , respectively, and x^n denotes any sequence $x_1 x_2 \cdots x_n$ in \mathcal{X}^n . We also define the rate of a linear code f to be the ratio n/m , and denote it by $R(f)$.

Note that any permutation (or interleaver) σ_n on n letters can be regarded as an automorphism on \mathcal{X}^n . We denote by Σ_n a uniformly distributed random permutation on n letters. We tacitly assume that different random permutations occurring in the same expression are independent.

Next, we introduce the concept of types [6]. The *type* of a sequence x^n in \mathcal{X}^n is the empirical distribution P_{x^n} on \mathcal{X} defined by

$$P_{x^n}(a) \triangleq \frac{1}{n} \sum_{i=1}^n 1\{x_i = a\} \quad \forall a \in \mathcal{X}$$

For a (probability) distribution P on \mathcal{X} , the set of sequences of type P in \mathcal{X}^n is denoted by $\mathcal{T}_P^n(\mathcal{X})$. A distribution P on \mathcal{X} is called a type of sequences in \mathcal{X}^n if $\mathcal{T}_P^n(\mathcal{X}) \neq \emptyset$. We denote by $\mathcal{P}(\mathcal{X})$ the set of all distributions on \mathcal{X} , and denote by $\mathcal{P}_n(\mathcal{X})$ the set of all possible types of sequences in \mathcal{X}^n .

Now, we introduce the *spectrum*, the most important concept in the code-spectrum approach. The spectrum of a nonempty set $A \subseteq \mathcal{X}^n$ is the empirical distribution $S_{\mathcal{X}}(A)$ on $\mathcal{P}(\mathcal{X})$ defined by

$$S_{\mathcal{X}}(A)(P) \triangleq \frac{|\{x^n \in A | P_{x^n} = P\}|}{|A|} \quad \forall P \in \mathcal{P}(\mathcal{X}).$$

Analogously, the *joint spectrum* of a nonempty set $B \subseteq \mathcal{X}^n \times \mathcal{Y}^m$ is the empirical distribution $S_{\mathcal{X}\mathcal{Y}}(B)$ on $\mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{Y})$

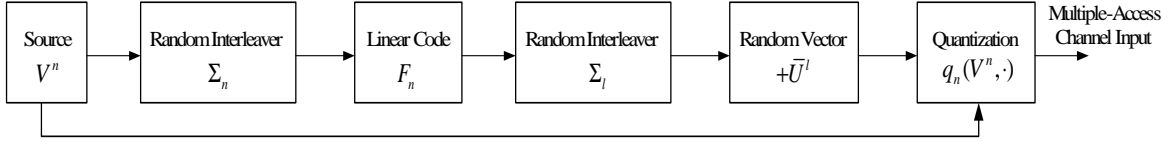


Fig. 1. The proposed linear codes based lossless joint source-channel encoding scheme of each encoder for multiple-access channels

defined by

$$S_{\mathcal{X}\mathcal{Y}}(B)(P, Q) \triangleq \frac{|\{(x^n, y^m) \in B | P_{x^n} = P, P_{y^m} = Q\}|}{|B|}$$

for all $P \in \mathcal{P}(\mathcal{X}), Q \in \mathcal{P}(\mathcal{Y})$. Furthermore, we define the *marginal spectra* $S_{\mathcal{X}}(B), S_{\mathcal{Y}}(B)$ as the marginal distributions of $S_{\mathcal{X}\mathcal{Y}}(B)$, that is,

$$S_{\mathcal{X}}(B)(P) \triangleq \sum_{Q \in \mathcal{P}(\mathcal{Y})} S_{\mathcal{X}\mathcal{Y}}(B)(P, Q)$$

$$S_{\mathcal{Y}}(B)(Q) \triangleq \sum_{P \in \mathcal{P}(\mathcal{X})} S_{\mathcal{X}\mathcal{Y}}(B)(P, Q).$$

Please note that the summation in the definition of $S_{\mathcal{X}}(B)(P)$ (or $S_{\mathcal{Y}}(B)(Q)$) is taken over an infinite set $\mathcal{P}(\mathcal{Y})$ (or $\mathcal{P}(\mathcal{X})$), but is actually over a finite set because

$$S_{\mathcal{X}\mathcal{Y}}(B)(P, Q) = 0$$

for any (P, Q) satisfying $P \in \mathcal{P}(\mathcal{X}) \setminus \mathcal{P}_n(\mathcal{X})$ or $Q \in \mathcal{P}(\mathcal{Y}) \setminus \mathcal{P}_m(\mathcal{Y})$. We define the *conditional spectra* $S_{\mathcal{Y}|\mathcal{X}}(B), S_{\mathcal{X}|\mathcal{Y}}(B)$ as the conditional distributions of $S_{\mathcal{X}\mathcal{Y}}(B)$, that is,

$$S_{\mathcal{Y}|\mathcal{X}}(B)(Q|P) \triangleq \frac{S_{\mathcal{X}\mathcal{Y}}(B)(P, Q)}{S_{\mathcal{X}}(B)(P)} \quad \forall P \text{ satisfying } S_{\mathcal{X}}(B)(P) \neq 0$$

$$S_{\mathcal{X}|\mathcal{Y}}(B)(P|Q) \triangleq \frac{S_{\mathcal{X}\mathcal{Y}}(B)(P, Q)}{S_{\mathcal{Y}}(B)(Q)} \quad \forall Q \text{ satisfying } S_{\mathcal{Y}}(B)(Q) \neq 0.$$

Then naturally, for any given function $f : \mathcal{X}^n \rightarrow \mathcal{Y}^m$, we can define its *joint spectrum* $S_{\mathcal{X}\mathcal{Y}}(f)$, *forward conditional spectrum* $S_{\mathcal{Y}|\mathcal{X}}(f)$, *backward conditional spectrum* $S_{\mathcal{X}|\mathcal{Y}}(f)$, and *image spectrum* $S_{\mathcal{Y}}(f)$ as $S_{\mathcal{X}\mathcal{Y}}(\text{rl}(f))$, $S_{\mathcal{Y}|\mathcal{X}}(\text{rl}(f))$, $S_{\mathcal{X}|\mathcal{Y}}(\text{rl}(f))$, and $S_{\mathcal{Y}}(\text{rl}(f))$, respectively, where $\text{rl}(f)$ is the *relation* defined by $\{(x^n, f(x^n)) | x^n \in \mathcal{X}^n\}$. In this case, the forward conditional spectrum is given by

$$S_{\mathcal{Y}|\mathcal{X}}(f)(Q|P) = \frac{S_{\mathcal{X}\mathcal{Y}}(f)(P, Q)}{S_{\mathcal{X}}(\mathcal{X}^n)(P)}.$$

If f is a linear code, we further define its *kernel spectrum* as $S_{\mathcal{X}}(\ker f)$, where $\ker f \triangleq \{x^n | f(x^n) = 0^m\}$. In this case, we have

$$S_{\mathcal{Y}}(f) = S_{\mathcal{Y}}(f(\mathcal{X}^n))$$

since f is a homomorphism according to the definition of linear codes.

The above definitions can be easily extended to more general cases. For example, we may consider the joint spectrum

$S_{\mathcal{X}\mathcal{Y}\mathcal{Z}}(C)$ of a set $C \subseteq \mathcal{X}^n \times \mathcal{Y}^m \times \mathcal{Z}^l$, or consider the joint spectrum $S_{\mathcal{X}_1\mathcal{X}_2\mathcal{Y}_1\mathcal{Y}_2}(g)$ of a function $g : \mathcal{X}_1^{n_1} \times \mathcal{X}_2^{n_2} \rightarrow \mathcal{Y}_1^{m_1} \times \mathcal{Y}_2^{m_2}$.

A series of properties regarding the spectrum of codes were proved in [4]. Readers may refer to [4] for the details. Some results are listed below for easy reference.

Proposition 2.1: For all $P \in \mathcal{P}_n(\mathcal{X})$ and $P_i \in \mathcal{P}_{n_i}(\mathcal{X}_i)$ ($1 \leq i \leq m$), we have

$$S_{\mathcal{X}}(\mathcal{X}^n)(P) = \frac{\binom{n}{nP}}{|\mathcal{X}|^n},$$

$$S_{\mathcal{X}_1 \dots \mathcal{X}_m}(\prod_{i=1}^m A_i)(P_1, \dots, P_m) = \prod_{i=1}^m S_{\mathcal{X}_i}(A_i)(P_i),$$

where

$$\binom{n}{nP} \triangleq \frac{n!}{\prod_{a \in \mathcal{X}} (nP(a))!}$$

and $A_i \subseteq \mathcal{X}_i^{n_i}$ ($1 \leq i \leq m$).

Proposition 2.2: For any given random function $F : \mathcal{X}^n \rightarrow \mathcal{Y}^m$, we have

$$\Pr\{\tilde{F}(x^n) = y^m\} = |\mathcal{Y}|^{-m} \alpha(F)(P_{x^n}, P_{y^m}) \quad (1)$$

for any $x^n \in \mathcal{X}^n, y^m \in \mathcal{Y}^m$, where

$$\tilde{F} \triangleq \Sigma_m \circ F \circ \Sigma_n \quad (2)$$

and

$$\begin{aligned} \alpha(F)(P, Q) &\triangleq \frac{E[S_{\mathcal{X}\mathcal{Y}}(F)(P, Q)]}{S_{\mathcal{X}\mathcal{Y}}(\mathcal{X}^n \times \mathcal{Y}^m)(P, Q)} \\ &= \frac{E[S_{\mathcal{Y}|\mathcal{X}}(F)(Q|P)]}{S_{\mathcal{Y}}(\mathcal{Y}^m)(Q)}. \end{aligned} \quad (3)$$

Proposition 2.3: For any given linear code $f : \mathcal{X}^n \rightarrow \mathcal{Y}^m$, we have

$$\alpha(f)(P_{0^n}, P_{y^m}) = |\mathcal{Y}|^m \mathbf{1}\{y^m = 0^m\}. \quad (4)$$

If both \mathcal{X} and \mathcal{Y} are the Galois field \mathbb{F}_q , we define a particular random linear code $F_{q,n,m}^{\text{RLC}} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ by $x^n \mapsto A_{m \times n} \cdot x^n$, where x^n represents an n -dimensional column vector, and $A_{m \times n}$ denotes a random matrix with m rows and n columns, each entry independently taking values in \mathbb{F}_q according to a uniform distribution on \mathbb{F}_q . (Note that for each realization of $A_{m \times n}$, we then obtain a corresponding realization of $F_{q,n,m}^{\text{RLC}}$. Such a random construction has already been adopted in [7, Section 2.1], [8], etc.) Then we have

$$\Pr\{\tilde{F}_{q,n,m}^{\text{RLC}}(x^n) = y^m\} = \Pr\{F_{q,n,m}^{\text{RLC}}(x^n) = y^m\} = q^{-m} \quad (5)$$

for all $x^n \in \mathbb{F}_q^n \setminus \{0^n\}$ and $y^m \in \mathbb{F}_q^m$, or equivalently

$$\alpha(F_{q,n,m}^{\text{RLC}})(P, Q) = 1 \quad (6)$$

for all $P \in \mathcal{P}_n(\mathbb{F}_q) \setminus \{P_{0^n}\}$ and $Q \in \mathcal{P}_m(\mathbb{F}_q)$.

III. SOME NEW RESULTS ABOUT CODE SPECTRA

In order to evaluate the performance of a linear code, we need to calculate or estimate its spectrum. However, the results established in [4] are still not enough for this purpose. So in this section, we will present some new results to facilitate the calculation of spectra. All the proofs are easy and hence omitted here.

First, we proved the following two propositions, which imply that any codes (or functions) may be regarded as conditional probability distributions. Such a viewpoint is very helpful when calculating the spectrum of a complex code consisting of many simple codes.

Proposition 3.1: For any random function $F : \mathcal{X}^n \rightarrow \mathcal{Y}^m$ and any $x^n \in \mathcal{X}^n$, we have

$$\Pr\{(F \circ \Sigma_n)(x^n) \in \mathcal{T}_Q^m(\mathcal{Y})\} = E[S_{\mathcal{Y}|\mathcal{X}}(F)(Q|P_{x^n})]. \quad (7)$$

Proposition 3.2: For any two random functions $F : \mathcal{X}^n \rightarrow \mathcal{Y}^m$ and $G : \mathcal{Y}^m \rightarrow \mathcal{Z}^l$, and any $O \in \mathcal{P}_n(\mathcal{X})$, $Q \in \mathcal{P}_l(\mathcal{Z})$, we have

$$\begin{aligned} & E[S_{\mathcal{Z}|\mathcal{X}}(G \circ \Sigma_m \circ F)(Q|O)] \\ &= \sum_{P \in \mathcal{P}_m(\mathcal{Y})} E[S_{\mathcal{Y}|\mathcal{X}}(F)(P|O)] E[S_{\mathcal{Z}|\mathcal{Y}}(G)(Q|P)]. \end{aligned}$$

Second, let us develop a generating function method for the calculations of spectra.

For any set $A \subseteq \mathcal{X}^n$, we define the *generating function* $\mathcal{G}(A)$ of its spectrum to be

$$\mathcal{G}(A)(u) \triangleq \sum_{P \in \mathcal{P}_n(\mathcal{X})} S_{\mathcal{X}}(A)(P)(u^{nP})_{\otimes}$$

where u is a map from \mathcal{X} to \mathbb{C} (the set of complex numbers) or $u \in \mathbb{C}^{\mathcal{X}}$, and for any $u, v \in \mathbb{C}^{\mathcal{X}}$, we define

$$(ru)(a) \triangleq ru(a) \quad \forall r \in \mathbb{C}, a \in \mathcal{X},$$

$$(u^v)(a) \triangleq u(a)^{v(a)} \quad \forall a \in \mathcal{X},$$

$$(u)_{\otimes} \triangleq \prod_{a \in \mathcal{X}} u(a).$$

Also note that $P \in \mathcal{P}_n(\mathcal{X}) \subseteq \mathbb{C}^{\mathcal{X}}$. Analogously, for any set $B \subseteq \mathcal{X}^n \times \mathcal{Y}^m$, we define the generating function of its joint spectrum as

$$\begin{aligned} \mathcal{G}(B)(u, v) &\triangleq \\ &\sum_{P \in \mathcal{P}_n(\mathcal{X}), Q \in \mathcal{P}_m(\mathcal{Y})} S_{\mathcal{X}\mathcal{Y}}(B)(P, Q)(u^{nP})_{\otimes} (v^{mQ})_{\otimes}, \end{aligned}$$

where $u \in \mathbb{C}^{\mathcal{X}}$, $v \in \mathbb{C}^{\mathcal{Y}}$. This in particular defines $\mathcal{G}(f) \triangleq \mathcal{G}(\text{rl}(f))$ for any function $f : \mathcal{X}^n \rightarrow \mathcal{Y}^m$.

Based on the above definitions, we proved the following properties.

Proposition 3.3: For any two sets $A_1 \subseteq \mathcal{X}^{n_1}$ and $A_2 \subseteq \mathcal{X}^{n_2}$, we have

$$\mathcal{G}(A_1 \times A_2)(u) = \mathcal{G}(A_1)(u) \cdot \mathcal{G}(A_2)(u). \quad (8)$$

For any two sets $A_1 \subseteq \mathcal{X}^n$ and $A_2 \subseteq \mathcal{Y}^m$, we have

$$\mathcal{G}(A_1 \times A_2)(u, v) = \mathcal{G}(A_1)(u) \cdot \mathcal{G}(A_2)(v). \quad (9)$$

For any two sets $B_1 \subseteq \mathcal{X}^{n_1} \times \mathcal{Y}^{m_1}$ and $B_2 \subseteq \mathcal{X}^{n_2} \times \mathcal{Y}^{m_2}$, we have

$$\mathcal{G}(B_1 \times B_2)(u, v) = \mathcal{G}(B_1)(u, v) \cdot \mathcal{G}(B_2)(u, v). \quad (10)$$

Corollary 3.1:

$$\mathcal{G}(\mathcal{X}^n)(u) = \left(\frac{(u)_{\oplus}}{|\mathcal{X}|} \right)^n,$$

where

$$(u)_{\oplus} \triangleq \sum_{a \in \mathcal{X}} u(a).$$

Corollary 3.2: For any two functions $f_1 : \mathcal{X}^{n_1} \rightarrow \mathcal{Y}^{m_1}$ and $f_2 : \mathcal{X}^{n_2} \rightarrow \mathcal{Y}^{m_2}$, we have

$$\mathcal{G}(f_1 \odot f_2)(u, v) = \mathcal{G}(f_1)(u, v) \cdot \mathcal{G}(f_2)(u, v), \quad (11)$$

where $f_1 \odot f_2$ is the map from $\mathcal{X}^{n_1+n_2}$ to $\mathcal{Y}^{m_1+m_2}$ defined by

$$(f_1 \odot f_2)(x^{n_1+n_2}) \triangleq f_1(x_{1 \dots n_1}) f_2(x_{(n_1+1) \dots (n_1+n_2)})$$

for all $x^{n_1+n_2} \in \mathcal{X}^{n_1+n_2}$.

IV. GENERAL PRINCIPLES FOR CONSTRUCTING LINEAR CODES WITH GOOD JOINT SPECTRA

In this section, we will investigate some general problems for constructing linear codes with good joint spectra.

At first, we need to introduce some concepts of good linear codes. According to [4, Table I], a sequence of δ -asymptotically good (random) linear codes $F_n : \mathcal{X}^n \rightarrow \mathcal{Y}^{m_n}$ for JSCC is a sequence of linear codes whose joint spectra satisfy

$$\limsup_{n \rightarrow \infty} \max_{P \in \mathcal{P}_n(\mathcal{X}) \setminus \{P_{0^n}\}, Q \in \mathcal{P}_{m_n}(\mathcal{Y})} \frac{1}{n} \ln \frac{E[S_{\mathcal{X}\mathcal{Y}}(F_n)(P, Q)]}{S_{\mathcal{X}\mathcal{Y}}(\mathcal{X}^n \times \mathcal{Y}^{m_n})(P, Q)} \leq \delta.$$

And for comparison, a sequence of δ -asymptotically good (random) linear codes $F_n : \mathcal{X}^n \rightarrow \mathcal{Y}^{m_n}$ for channel coding is a sequence of linear codes whose image spectra satisfy

$$\limsup_{n \rightarrow \infty} \max_{Q \in \mathcal{P}_{m_n}(\mathcal{Y}) \setminus \{P_{0^{m_n}}\}} \frac{1}{m_n} \ln \frac{E[S_{\mathcal{Y}}(F_n(\mathcal{X}^n))(Q)]}{S_{\mathcal{Y}}(\mathcal{Y}^{m_n})(Q)} \leq \delta.$$

When δ equals zero, the above codes are then called asymptotically good linear codes for JSCC and channel coding, respectively.

From the linearity of codes, it follows easily that δ -asymptotically good linear codes for JSCC are subsets of $\delta \bar{R}(\mathbf{F})$ -asymptotically good linear codes for channel coding, where $\bar{R}(\mathbf{F}) \triangleq \limsup_{n \rightarrow \infty} R(F_n)$ and $\mathbf{F} \triangleq \{F_n\}_{n=1}^{\infty}$. Then naturally, our *first problem* is: if a sequence of asymptotically good linear codes f_n for channel coding is given, can we find a sequence of asymptotically good linear codes g_n for JSCC

such that $g_n(\mathcal{X}^n) = f_n(\mathcal{X}^n)$? In other words (assuming that $\mathcal{X} = \mathcal{Y} = \mathbb{F}_q$), if a sequence of asymptotically good channel codes is given, can we choose a good sequence of generator matrices so that the linear codes are asymptotically good for JSCC?

When $\mathcal{X} = \mathbb{F}_q$, the answer is positive, as a consequence of the following theorem.

Theorem 4.1: For any linear code $f : \mathbb{F}_q^n \rightarrow \mathcal{Y}^m$, there exists a linear code $g : \mathbb{F}_q^n \rightarrow \mathcal{Y}^m$ such that

$$g(\mathbb{F}_q^n) = f(\mathbb{F}_q^n)$$

and

$$S_{\mathcal{Y}|\mathbb{F}_q}(g)(Q|P) < \frac{S_{\mathcal{Y}}(f(\mathbb{F}_q^n))(Q)}{1 - q^{-1} - q^{-2}} \quad (12)$$

for all $P \in \mathcal{P}_n(\mathbb{F}_q) \setminus \{P_{0^n}\}$, $Q \in \mathcal{P}_m(\mathcal{Y})$.

Proof: [Sketch of Proof] The main idea of the proof is to construct a random linear code $G \triangleq f \circ F_{q,n,n}^{\text{RLC}} \triangleq f \circ \Sigma_n \circ F_{q,n,n}^{\text{RLC}}$, where $F_{q,n,n}^{\text{RLC}}$ is defined in Proposition 2.3. Then by Proposition 3.2, we have $E[S_{\mathcal{Y}|\mathbb{F}_q}(G)(Q|P)] = S_{\mathcal{Y}}(f(\mathbb{F}_q^n))(Q)$ for all $P \neq P_{0^n}$ and Q . This together with Proposition 4.1 (see below) then concludes the theorem. \square

Proposition 4.1: Let $\text{rank}(F)$ be the rank of the generator matrix of the linear code $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$. Then we have

$$\Pr\{\text{rank}(F_{q,n,m}^{\text{RLC}}) = m\} = \prod_{i=1}^m \left(1 - \frac{q^{i-1}}{q^n}\right) \quad (13)$$

where $F_{q,n,m}^{\text{RLC}}$ is defined in Proposition 2.3 and $m \leq n$. Furthermore, we have

$$\prod_{i=1}^m \left(1 - \frac{q^{i-1}}{q^n}\right) > \left(1 - \frac{q^{m-n-k}}{q-1}\right) \prod_{i=1}^k \left(1 - \frac{q^{m-n-i}}{q^n}\right), \quad (14)$$

where $1 \leq k \leq m$. Let $m = n$ and $k = 1$, then we have

$$\Pr\{\text{rank}(F_{q,n,n}^{\text{RLC}}) = n\} > 1 - q^{-1} - q^{-2}. \quad (15)$$

Proof: The identity (13) is a well known result in probability theory. To obtain a lower bound of the right hand side of (13), we have

$$\begin{aligned} \prod_{i=1}^m \left(1 - \frac{q^{i-1}}{q^n}\right) &= \prod_{i=1}^{m-k} \left(1 - \frac{q^{i-1}}{q^n}\right) \prod_{i=1}^k \left(1 - \frac{q^{m-i}}{q^n}\right) \\ &\geq \left(1 - \sum_{i=1}^{m-k} \frac{q^{i-1}}{q^n}\right) \prod_{i=1}^k \left(1 - \frac{q^{m-i}}{q^n}\right) \\ &= \left(1 - \frac{q^{m-k} - 1}{q^n(q-1)}\right) \prod_{i=1}^k \left(1 - \frac{q^{m-i}}{q^n}\right) \\ &> \left(1 - \frac{q^{m-n-k}}{q-1}\right) \prod_{i=1}^k \left(1 - \frac{q^{m-i}}{q^n}\right). \end{aligned}$$

This concludes (14), and (15) follows clearly. \square

The above result does give a possible way for constructing good linear codes for JSCC based on good channel codes. However, such a construction is somewhat difficult to implement in practice, because the random generator matrix of $F_{q,n,m}^{\text{RLC}}$ is dense. Thus, our *second problem* is how to construct

linear codes with good joint spectra based on sparse matrices so that known iterative encoding and decoding procedures have low complexity. The following theorem gives one feasible solution.

Theorem 4.2: For a given sequence of sets $\{A_n \subseteq \mathcal{P}_{m_n}(\mathcal{X}) \setminus \{P_{0^{m_n}}\}\}_{n=1}^\infty$, if there exist two sequences of random linear codes $F_n : \mathcal{X}^n \rightarrow \mathcal{X}^{m_n}$ and $G_n : \mathcal{X}^{m_n} \rightarrow \mathcal{X}^{l_n}$ satisfying

$$F_n(\mathcal{X}^n \setminus \{0^n\}) \subseteq \bigcup_{P \in A_n} \mathcal{T}_P^{m_n}(\mathcal{X}) \quad (16)$$

and

$$\limsup_{n \rightarrow \infty} \max_{P \in A_n, Q \in \mathcal{P}_{l_n}(\mathcal{X})} \frac{1}{n} \ln \frac{E[S_{\mathcal{X}|\mathcal{X}}(G_n)(Q|P)]}{S_{\mathcal{X}}(\mathcal{X}^{l_n})(Q)} \leq \delta \quad (17)$$

respectively, where $\delta \geq 0$, then we have

$$\limsup_{n \rightarrow \infty} \max_{O \in \mathcal{P}_n(\mathcal{X}) \setminus \{P_{0^n}\}, Q \in \mathcal{P}_{l_n}(\mathcal{X})} \frac{1}{n} \ln \frac{E[S_{\mathcal{X}|\mathcal{X}}(G_n \circ \Sigma_{m_n} \circ F_n)(Q|O)]}{S_{\mathcal{X}}(\mathcal{X}^{l_n})(Q)} \leq \delta.$$

Proof: For all $O \in \mathcal{P}_n(\mathcal{X}) \setminus \{P_{0^n}\}$ and $Q \in \mathcal{P}_{l_n}(\mathcal{X})$, and for any $\epsilon > 0$ and sufficiently large n , we have

$$\begin{aligned} &S_{\mathcal{X}|\mathcal{X}}(G_n \circ \Sigma_{m_n} \circ F_n)(Q|O) \\ &\stackrel{(a)}{=} \sum_{P \in \mathcal{P}_{m_n}(\mathcal{X})} E[S_{\mathcal{X}|\mathcal{X}}(G_n)(Q|P)] E[S_{\mathcal{X}|\mathcal{X}}(F_n)(P|O)] \\ &\stackrel{(b)}{=} \sum_{P \in A_n} E[S_{\mathcal{X}|\mathcal{X}}(G_n)(Q|P)] E[S_{\mathcal{X}|\mathcal{X}}(F_n)(P|O)] \\ &\stackrel{(c)}{\leq} \sum_{P \in A_n} e^{n(\delta+\epsilon)} S_{\mathcal{X}}(\mathcal{X}^{l_n})(Q) E[S_{\mathcal{X}|\mathcal{X}}(F_n)(P|O)] \\ &\leq e^{n(\delta+\epsilon)} S_{\mathcal{X}}(\mathcal{X}^{l_n})(Q), \end{aligned}$$

where (a) follows from Proposition 3.2, (b) from the condition (16), and (c) from the condition (17). Therefore, for any $\epsilon > 0$ and sufficiently large n ,

$$\max_{O \in \mathcal{P}_n(\mathcal{X}) \setminus \{P_{0^n}\}, Q \in \mathcal{P}_{l_n}(\mathcal{X})} \frac{1}{n} \ln \frac{E[S_{\mathcal{X}|\mathcal{X}}(G_n \circ \Sigma_{m_n} \circ F_n)(Q|O)]}{S_{\mathcal{X}}(\mathcal{X}^{l_n})(Q)} \leq \delta + \epsilon,$$

which establishes the theorem. \square

Using Theorem 4.2, we can now construct good linear codes by a serial concatenation scheme, where the inner code is approximately δ -asymptotically good (satisfying (17)) and the outer code is a linear code having good distance properties if we set $A_n = \{P \in \mathcal{P}_{m_n}(\mathcal{X}) | 1 - P(0) > \gamma\}$ in the condition (16). According to [9, Section IV], there exists a good low density parity check (LDPC) code F_n satisfying (16) for an appropriate γ . Then our *final problem* is how to find a sequence of approximately δ -asymptotically good linear codes satisfying (17) with $A_n = \{P \in \mathcal{P}_{m_n}(\mathcal{X}) | 1 - P(0) > \gamma\}$. In the next section, we will find such codes in a family of codes called low density generator matrix (LDGM) codes.

V. THE SPECTRA OF LDGM CODES

In this section, we will investigate the joint spectra of LDGM codes. We assume that the alphabet of codes is \mathbb{F}_q , and we denote a regular LDGM code by the map $F_{n,c,d}^{\text{LD}} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ defined by

$$F_{n,c,d}^{\text{LD}} \triangleq (\odot_{i=1}^m F_d^{\text{CHK}}) \circ \Sigma_{cn} \circ (\odot_{i=1}^n f_c^{\text{REP}})$$

where $nc = md$, and f_c^{REP} is a single symbol repetition code $f_c^{\text{REP}} : \mathbb{F}_q \rightarrow \mathbb{F}_q^c$ defined by

$$f_c^{\text{REP}}(x) \triangleq xx \cdots x \quad \forall x \in \mathbb{F}_q,$$

and $\odot_{i=1}^m F_d^{\text{CHK}}$ denotes a parallel concatenation of m independent copies of the random single symbol check code $F_d^{\text{CHK}} : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ defined by

$$F_d^{\text{CHK}}(x^d) \triangleq \sum_{i=1}^d C_i x_i \quad \forall x^d \in \mathbb{F}_q^d$$

where C_i ($i = 1, 2, \dots, d$) denotes an independent uniform random variable on the set $\mathbb{F}_q \setminus \{0\}$.

To evaluate the joint spectrum or conditional spectrum of $F_{n,c,d}^{\text{LD}}$, we first need to calculate the joint spectrum or conditional spectrum of f_c^{REP} and F_d^{CHK} . We have the following results.

Proposition 5.1:

$$\mathcal{G}(f_c^{\text{REP}})(u, v) = \frac{1}{q} \sum_{a \in \mathbb{F}_q} u(a)[v(a)]^c, \quad (18)$$

$$\begin{aligned} \mathcal{G}(\odot_{i=1}^n f_c^{\text{REP}})(u, v) \\ = \frac{1}{q^n} \sum_{P \in \mathcal{P}_n(\mathbb{F}_q)} \binom{n}{nP} (u^{nP})_{\otimes} (v^{ncP})_{\otimes}, \end{aligned} \quad (19)$$

$$S_{\mathbb{F}_q \mathbb{F}_q}(\odot_{i=1}^n f_c^{\text{REP}})(P, Q) = S_{\mathbb{F}_q}(\mathbb{F}_q^n)(P) 1\{P = Q\}, \quad (20)$$

$$S_{\mathbb{F}_q \mathbb{F}_q}(\odot_{i=1}^n f_c^{\text{REP}})(Q|P) = 1\{P = Q\}. \quad (21)$$

Proof: The identity (18) holds clearly. From (18) and Corollary 3.2, we then have

$$\begin{aligned} \mathcal{G}(\odot_{i=1}^n f_c^{\text{REP}})(u, v) \\ = \left(\frac{1}{q} \sum_{a \in \mathbb{F}_q} u(a)[v(a)]^c \right)^n \\ = \frac{1}{q^n} \sum_{P \in \mathcal{P}_n(\mathbb{F}_q)} \binom{n}{nP} \prod_{a \in \mathbb{F}_q} [u(a)]^{nP(a)} [v(a)]^{ncP(a)} \\ = \frac{1}{q^n} \sum_{P \in \mathcal{P}_n(\mathbb{F}_q)} \binom{n}{nP} (u^{nP})_{\otimes} (v^{ncP})_{\otimes}. \end{aligned}$$

This proves (19). The identities (20) and (21) are easy consequences of (19). \square

In order to obtain the joint spectrum of F_d^{CHK} , we need the following proposition (also well known), which can be easily proved by mathematical induction.

Proposition 5.2: Let

$$Y_d = \sum_{i=1}^d X_i, \quad (22)$$

where X_i ($i = 1, 2, \dots, d$) is an independent uniform random variable on the set $\mathbb{F}_q \setminus \{0\}$. Then we have

$$\begin{aligned} \Pr\{Y_d = a\} &= 1\{a = 0\} \frac{1}{q} \left[1 - \left(-\frac{1}{q-1} \right)^{d-1} \right] + \\ &1\{a \neq 0\} \frac{1}{q} \left[1 - \left(-\frac{1}{q-1} \right)^d \right] \end{aligned} \quad (23)$$

for any $a \in \text{GF}(q)$.

Now let us calculate the joint spectrum of F_d^{CHK} . By Proposition 2.2, 5.2 and Corollary 3.2, we obtained the following proposition. Its proof is long and hence omitted here, and readers may refer to [10] for the details.

Proposition 5.3:

$$\begin{aligned} E[\mathcal{G}(F_d^{\text{CHK}})(u, v)] &= \frac{1}{q^{d+1}} \left[((u)_{\oplus})^d (v)_{\oplus} + \right. \\ &\left. \left(\frac{qu(0) - (u)_{\oplus}}{q-1} \right)^d (qv(0) - (v)_{\oplus}) \right], \end{aligned} \quad (24)$$

$$E[S_{\mathbb{F}_q \mathbb{F}_q}(\odot_{i=1}^m F_d^{\text{CHK}})(P, Q)] = \text{coef}(g_1(u, Q), (u^{mdP})_{\otimes}), \quad (25)$$

$$\begin{aligned} E[S_{\mathbb{F}_q \mathbb{F}_q}(\odot_{i=1}^m F_d^{\text{CHK}})(P, Q)] &\leq g_2(O, P, Q), \\ \forall O \in \mathcal{P}_{md}(\mathbb{F}_q) \quad (O(a) > 0, \forall a \in \{a | P(a) > 0\}), \end{aligned} \quad (26)$$

$$\frac{1}{m} \ln \alpha(\odot_{i=1}^m F_d^{\text{CHK}})(P, Q) \leq \delta_d(P(0), Q(0)) + O\left(\frac{\ln m}{m}\right), \quad (27)$$

where $\text{coef}(f(u), (u^v)_{\otimes})$ denotes the coefficient of $(u^v)_{\otimes}$ in the polynomial $f(u)$, and

$$\begin{aligned} g_1(u, Q) \\ \triangleq \frac{\binom{m}{mQ}}{q^{m(d+1)}} \left[((u)_{\oplus})^d + (q-1) \left(\frac{qu(0) - (u)_{\oplus}}{q-1} \right)^d \right]^{mQ(0)} \\ \left[((u)_{\oplus})^d - \left(\frac{qu(0) - (u)_{\oplus}}{q-1} \right)^d \right]^{m(1-Q(0))}, \end{aligned}$$

$$\begin{aligned} g_2(O, P, Q) \\ \triangleq \frac{\binom{m}{mQ}}{q^{m(d+1)} (O^{mdP})_{\otimes}} \left[1 + (q-1) \left(\frac{qO(0) - 1}{q-1} \right)^d \right]^{mQ(0)} \\ \left[1 - \left(\frac{qO(0) - 1}{q-1} \right)^d \right]^{m(1-Q(0))}, \end{aligned}$$

$$\begin{aligned} \delta_d(x, y) &\triangleq \inf_{0 < \hat{x} < 1} \left\{ dD(x \| \hat{x}) + y \ln \left[1 + (q-1) \left(\frac{q\hat{x} - 1}{q-1} \right)^d \right] \right. \\ &\quad \left. + (1-y) \ln \left[1 - \left(\frac{q\hat{x} - 1}{q-1} \right)^d \right] \right\}. \end{aligned} \quad (28)$$

where $D(x \| \hat{x})$ is the *information divergence* defined by

$$D(x \| \hat{x}) \triangleq x \ln \frac{x}{\hat{x}} + (1-x) \ln \frac{1-x}{1-\hat{x}}.$$

Based on the above preparations, we now start to analyze the joint spectrum of the regular LDGM code $F_{n,c,d}^{\text{LD}}$.

Theorem 5.1:

$$\frac{1}{n} \ln \alpha(F_{n,c,d}^{\text{LD}})(P, Q) \leq \frac{c}{d} \delta_d(P(0), Q(0)) + O\left(\frac{\ln n}{n}\right). \quad (29)$$

where δ_d is defined by (28). Let

$$A_n(\gamma) \triangleq \{P \in \mathcal{P}_n(\mathbb{F}_q) | 1 - P(0) > \gamma\}, \quad (30)$$

where $0 < \gamma < 1$. Then, when $q > 2$, for any $0 < \gamma < 1$ and any $\delta > 0$, there exists a positive integer $d_0 = d_0(\gamma, \delta)$ such that

$$\limsup_{n \rightarrow \infty} \max_{P \in A_n(\gamma), Q \in \mathcal{P}_m(\mathbb{F}_q)} \frac{1}{n} \ln \alpha(F_{n,c,d}^{\text{LD}})(P, Q) \leq \delta \quad (31)$$

for all integers $d \geq d_0$.

Proof: At first, according to the definition of regular LDGM codes, we have

$$\begin{aligned} & E[S_{\mathbb{F}_q|\mathbb{F}_q}(F_{n,c,d}^{\text{LD}})(Q|P)] \\ \stackrel{(a)}{=} & \sum_{O \in \mathcal{P}_{nc}(\mathbb{F}_q)} E[S_{\mathbb{F}_q|\mathbb{F}_q}(\odot_{i=1}^n f_c^{\text{REP}})(O|P)] \cdot \\ & E[S_{\mathbb{F}_q|\mathbb{F}_q}(\odot_{i=1}^m F_d^{\text{CHK}})(Q|O)] \\ \stackrel{(b)}{=} & \sum_{O \in \mathcal{P}_{nc}(\mathbb{F}_q)} 1\{P = O\} E[S_{\mathbb{F}_q|\mathbb{F}_q}(\odot_{i=1}^m F_d^{\text{CHK}})(Q|O)] \\ = & E[S_{\mathbb{F}_q|\mathbb{F}_q}(\odot_{i=1}^m F_d^{\text{CHK}})(Q|P)] \\ \stackrel{(c)}{\leq} & e^{m(\delta_d(P(0), Q(0)) + O(\frac{\ln m}{m}))} S_{\mathbb{F}_q}^m(\mathbb{F}_q^m)(Q), \end{aligned}$$

where (a) follows from Proposition 3.2 and the definition of $F_{n,c,d}^{\text{LD}}$, (b) from Proposition 5.1, and (c) from Proposition 5.3. This then concludes (29).

By the definition of δ_d , we have

$$\begin{aligned} \delta_d(x, y) & \leq dD(x||x) + y \ln \left[1 + (q-1) \left(\frac{qx-1}{q-1} \right)^d \right] \\ & \quad + (1-y) \ln \left[1 - \left(\frac{qx-1}{q-1} \right)^d \right] \\ & \leq \ln \left[1 + (qy-1) \left(\frac{qx-1}{q-1} \right)^d \right] \\ & \leq (qy-1) \left(\frac{qx-1}{q-1} \right)^d \\ & \leq (q-1) \left| \frac{qx-1}{q-1} \right|^d. \end{aligned}$$

Furthermore, when $0 \leq x < 1 - \gamma$ and $q > 2$, we have

$$-1 < -\frac{1}{q-1} \leq \frac{qx-1}{q-1} \leq 1 - \frac{q\gamma}{q-1} < 1$$

or

$$\left| \frac{qx-1}{q-1} \right| < \max\left\{ \frac{1}{q-1}, 1 - \frac{q\gamma}{q-1} \right\} < 1.$$

Then there exists a positive integer $d_0 = d_0(\gamma, \delta)$ such that

$$\sup_{\substack{0 \leq x < 1-\gamma, \\ 0 \leq y \leq 1}} \delta_d(x, y) \leq \frac{d\delta}{c} \quad \forall d \geq d_0.$$

Note here that the ratio d/c is the rate of the code and hence should be a constant or at least bounded.

Therefore, for any $d \geq d_0$, we have

$$\begin{aligned} & \max_{P \in A_n(\gamma), Q \in \mathcal{P}_m(\mathbb{F}_q)} \frac{1}{n} \ln \alpha(F_{n,c,d}^{\text{LD}})(P, Q) \\ \stackrel{(a)}{\leq} & \frac{c}{d} \sup_{\substack{0 \leq x < 1-\gamma, \\ 0 \leq y \leq 1}} \delta_d(x, y) + O\left(\frac{\ln n}{n}\right) \\ \leq & \delta + O\left(\frac{\ln n}{n}\right), \end{aligned}$$

where (a) follows from (29). This concludes (31). \square

Theorem 5.1 actually exhibits a family of codes whose joint spectra are approximately δ -asymptotically good. Then together with the conclusion at the end of Section IV, we have completed the construction of linear codes with good joint spectra, i.e., a serial concatenation scheme with one LDPC code as an outer code and one LDGM code as an inner code. An analogous construction has been proposed by Hsu in his thesis [11], but his purpose was only to find good channel codes and only a rate-1 LDGM code was employed as an inner code in his construction.

REFERENCES

- [1] Y. Zhao and J. Garcia-Frias, "Turbo compression/joint source-channel coding of correlated binary sources with hidden Markov correlation," *Signal Processing*, vol. 86, no. 11, pp. 3115–3122, 2006.
- [2] J. Garcia-Frias, Y. Zhao, and W. Zhong, "Turbo-like codes for transmission of correlated sources over noisy channels," *IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 58–66, Sep. 2007.
- [3] Y. Zhao, W. Zhong, and J. Garcia-Frias, "Transmission of correlated senders over a Rayleigh fading multiple access channel," *Signal Processing*, vol. 86, no. 11, pp. 3150–3159, 2006.
- [4] S. Yang, Y. Chen, and P. Qiu, "Linear codes based lossless joint source-channel coding for multiple-access channels," submitted to *IEEE Trans. Inf. Theory*, draft available at <http://arxiv.org/abs/cs.IT/0611146>.
- [5] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for "Turbo-like" codes," in *36th Allerton Conf. on Communication, Control, and Computing*, Sep. 1998, pp. 201–210.
- [6] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic Press, 1981.
- [7] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
- [8] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Trans. Inf. Theory*, vol. 28, no. 4, pp. 585–592, Jul. 1982.
- [9] A. Bennatan and D. Burshtein, "On the application of LDPC codes to arbitrary discrete-memoryless channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 417–437, Mar. 2004.
- [10] S. Yang, et al, "Constructing linear codes with good spectra," in preparation, to be submitted to *IEEE Trans. Inf. Theory*.
- [11] C.-H. Hsu, "Design and analysis of capacity-achieving codes and optimal receivers with low complexity," Ph.D. dissertation, University of Michigan, 2006.